IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. HAOYANG YU, *et al*.	No. 19-cr-10195-WGY

MEMORANDUM IN SUPPORT OF
MOTION TO SUPPRESS EVIDENCE FROM WARRANTLESS SEARCH
AND REQUEST FOR EVIDENTIARY HEARING

William W. Fick (BBO #650562)
Daniel N. Marx (BBO #674523)
Amy Barsky (BBO #601111)
FICK & MARX LLP
24 Federal Street, 4th Floor
Boston, MA 02110
(857) 321-8360
wfick@fickmarx.com
dmarx@fickmarx.com
abarsky@fickmarx.com

Dated: June 22, 2020

TABLE OF CONTENTS

BACKGROUND

On June 11, 2019, Defendant Haoyang Yu was charged in a 15-count indictment with various trade secret offenses: stealing trade secrets in violation of 18 U.S.C. § 1832(a)(1) & (a)(4); copying, uploading, or downloading trade secrets in violation of § 1832(a)(2) & (a)(4); and possessing trade secrets in violation of § 1832(a)(3) & (a)(4). *See* DE #1 (Counts I-XIV). Mr. Yu allegedly misappropriated from his former employer, Analog Devices, Inc. ("ADI" or "Analog"), data and other materials about monolithic microwave integrated circuits ("MMICs"), a common circuit found in many electronic devices. Mr. Yu. was also charged with "smuggling" in violation of 18 U.S.C. § 554, because he allegedly shipped certain MMIC products to a commercial customer in Spain. *See id.* (Count XV).

A. Mr. Yu's employment with ADI

On July 21, 2014, Mr. Yu joined Hittite Microwave Corp., which was later acquired by Analog Devices, Inc. ("ADI" or "Analog"), as a Principal Engineer. *See* Declaration of Haoyang Yu (June 9, 2020) ("Yu Decl.") ¶ 2. As of 2017, Mr. Yu reported directly to Tariq Lodhi and ultimately to Bob Broughton. *See id.* ¶ 3.

At all relevant times, ADI had monitoring software, known as Digital Guardian, that gave ADI the capacity to conduct extensive historical searches of employees' computers, e-mails, and network activity, including by monitoring all downloads, uploads, and printouts. *See* Ex. A (DOJ-YU-0000060-66); *see generally* https://digitalguardian.com/solutions/data-visibility (last visited June 9, 2020) ("Digital Guardian delivers the broadest and deepest data visibility for information security professionals. Regardless of where the data resides, endpoints, shares, databases, or in the cloud, Digital Guardian can locate and track the movement of your sensitive data. Our agent provides complete visibility to all hardware, software, data creation, data storage and data movement.").

As an employee of ADI, Mr. Yu expected that his data and communications at work would remain private and that ADI would not closely monitor his computer, email, or network activity, by activating Digital Guardian or similar surveillance technology, without giving him advance notice. *See* Yu Decl. ¶ 7. At no time, did anyone at ADI tell Mr. Yu that it was using Digital Guardian or any other software to monitor his activities or data. *See id.* ¶ 8.

B. ADI's Implementation of Digital Guardian to Monitor Mr. Yu

In or about October 2016, at Broughton's request and without notice to Mr. Yu, ADI "implement[ed]" Digital Guardian to monitor Mr. Yu and another Chinese American employee. *See* Ex. A; Ex. B (ADI-YU-00000408). Broughton had never previously activated Digital Guardian for any other ADI employee, *see id.*, and no one informed Mr. Yu that ADI had started monitoring his computer, email, and network activity, *see* Yu Decl. ¶ 8. Thereafter, "every week or two," employees in ADI's HR department checked for any suspicious file downloads by Mr. Yu, but they found "*[n]o sign of unusual activity*." Ex. C (ADI-YU-00000439-40) (emphasis added).

In July 2017, Broughton falsely accused Mr. Yu of stealing ADI property. *See* Yu Decl. ¶ 5; Ex. D (ADI-YU-00000443). A colleague saw Mr. Yu carrying a box of papers to his car, but upon further investigation, all those materials proved to be "personal" (as Mr. Yu had told Broughton and Lodhi). *See* Yu Decl. ¶ 5; Ex. E (ADI-YU-00000447-48 (Lodhi: "I confirmed the items in his car were personal."). Further, Broughton was again told that, although ADI had been "monitoring" Mr. Yu's computer "for some time," Digital Guardian reports revealed "*no suspicious activity*." Ex. F (ADI-YU-0000446) (emphasis added).

Effective August 4, 2017, Mr. Yu resigned from ADI. *See* Yu Decl. ¶ 6. Around the time of Mr. Yu's departure, ADI did not generate, obtain, or review any detailed information from

Digital Guardian concerning Mr. Yu's use of ADI's devices or systems. Nor did ADI conduct any forensic investigation of Mr. Yu's computer, e-mail, or network activity.

C. ADI's warrantless search of Mr. Yu's data, at the government's behest

In April 2018, government investigators met with ADI representatives concerning a then-pending federal investigation into whether Mr. Yu and his company, Tricon MMIC, were selling export-controlled products to Chinese entities without required licenses. *See* Ex. G (DOJ-YU-000036).

During a meeting on April 23, 2018, which was attended by ADI representatives (including in-house and outside counsel), agents from the Department of Commerce (Bureau of Industry and Security), Department of Homeland Security (Homeland Security Investigations), and Federal Bureau of Investigation, as well as the Assistant U.S. Attorney who is currently prosecuting this case, ADI first told government agents that the company "use[s] software called digital guardian that tracks [its] employee's movement on [ADI] computers." *Id.*

At some point after that initial meeting, government investigators "tasked" Broughton with "gather[ing] information for investigators" from Digital Guardian about Mr. Yu. *See* Ex. A. Before the investigators directed ADI to search that data, Broughton had only "limited access" to any such information, which was "considered a Human Resources personnel matter," and had not been gathered by ADI for any business purpose. *Id.*

At a subsequent meeting, on May 10, 2018, Broughton presented investigators with detailed data and information concerning Mr. Yu that ADI had recently gathered from Digital Guardian. *See id.* (and corresponding presentation slides). Those materials have been used, and will continue to be used, in the prosecution of Mr. Yu.

The collaboration between the government and ADI was not limited to collecting information from Digital Guardian. In fact, ADI's involvement in the government's investigation

was long-running and substantial. For example, or around June 7, 2018, rather than enlisting a government-employed or independent expert, law enforcement agents provided ADI employees with samples of Tricon products, and together, they "test[ed]" and analyzed of those products. *See* Ex. H (DOJ-YU-000038-46).

ARGUMENT

When ADI used sophisticated monitoring software to conduct an extensive digital search of Mr. Yu's computer, email, and network activity, at the government's request, ADI acted as a government agent and, thus, should have obtained a warrant. Because Mr. Yu had a reasonable expectation of privacy in his electronic devices and activities, while working as an ADI employee, the warrantless search was unreasonable, and all fruits of that search should be suppressed.

I. ADI acted as a government agent, for Fourth Amendment purposes, when it conducted a warrantless search of Mr. Yu's computer, email, and network activity.

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." U.S. Const., 4th amend. Although that constitutional protection is limited to "government action," it bars unreasonable searches by a private entity or individual who acts as "an agent of the Government or with the participation or knowledge of any government official." *United States v. Momoh*, 427 F.3d 137, 140 (1st Cir. 2005) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)); *see United States v. D'Andrea*, 648 F.3d 1, 10 (1st Cir. 2011) (holding "a search carried out by a private party in conjunction with government efforts may no longer qualify as a private search immune from the Fourth Amendment"). In this case, ADI acted as a government agent when, at the government's behest, it conducted a warrantless search of Mr. Yu's computer, email, and network activity.

A. The First Circuit has identified several factors to determine when a private actor serves as a government agent.

The First Circuit has identified the following three factors as "potentially relevant" in deciding whether, for Fourth Amendment purposes, a private party acts as a government agent: "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent which the private party aims primarily to help the government or to serve its own interests." *United States v. Silva*, 554 F.3d 13, 18 (1st Cir. 2009) (*United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997)).

These three factors are only helpful guideposts, however, because "there is a grey area between overt Government participation and complete absence of participation that should be resolved on a case-by-case basis." *United States v. Montes*, No. 06-cr-009, 2011 U.S. Dist. LEXIS 47141, at *28-29 (D.P.R. May 2, 2011) (citing *United States v. Walther*, 652 F.2d 788, 791 (9th Cir. 1981)).

Notably, the government's stated position about a private party's search is not dispositive of this Court's analysis. *See United States v. Montes*, No. 06-cr-009 (JAG), 2011 U.S. Dist. LEXIS 47046, at *50 (D.P.R. Feb. 28, 2011) ("A disclaimer by the government that the informant want not a government agent would still not preclude finding that the informant was acting as [a] government agent when he elicited the statement.").

B. The government instigated and participated in the warrantless search by ADI.

The key factor, according to the First Circuit, is whether government agents have "instigated" or "participated" in a private search. *See Momoh*, 427 F.3d at 140-41 (citing *Pervaz*, 118 F.3d at 6). In this context, "'instigating' . . . properly means 'affirmative encouragement,'" *id.* at 141 (citing *United States v. Smythe*, 84 F.3d 1240, 1243 (10th Cir. 1996)), and includes "directing" a search, *id.* (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971)). In *Momoh*,

for example, no government search occurred, because DHL opened the defendant's outbound, international package pursuant to general FAA regulations (not at the specific request of any FAA investigators) and before DHL communicated with any government agents.

Here, in contrast, ADI searched data from Digital Guardian concerning Mr. Yu's devices and activities *only after the FBI expressly asked ADI to conduct that search*. And ADI had no other business purpose; if the company had any private interest in gathering and searching Digital Guardian data, it would have taken those steps around the time when Mr. Yu ended his employment. For nearly one year, however, ADI did not bother to look, because it had no independent reason to do so.

C. An evidentiary hearing is required to assess the government's role in ADI's warrantless search.

Given the "fact-dependent nature of this inquiry," it is appropriate to hold an evidentiary hearing, especially when critical evidence is uniquely in the possession of the government or a third-party (here, ADI). *United States v. Gaudette*, No. 09-cr-30014-MAP, 2011 U.S. Dist. LEXIS 84, at *16 (D. Mass. Jan. 3, 2011). Indeed, it is reversible error to deny a suppression motion without an evidentiary hearing, where "under the factors enunciated in *Pervaz* and its progeny," an informant's search of a defendant's property "amounted to a government search and not a private search." *D'Andrea*, 648 F.3d at 10 (vacating denial of suppression motion and remanding for evidentiary hearing).

This case resembles *United States v. Gaudette*, No. 09-cr-30014-MAP, 2011 U.S. Dist. LEXIS 84, at *16-17 (D. Mass. Jan. 3, 2011), where government agents asked an electric company employee to check the electric meter at a private residence where a suspect was believed to be running an indoor marijuana growing operation. The court ordered an evidentiary hearing on the defendant's claim that, when the electronic company employee viewed his meter to determine the

usage (and whether the meter had been altered), "her observations amounted to government action, requiring her to obtain a warrant before entering the property," because a police investigator had "requested" that she conduct that check. *See id.*

Ultimately, in *Gaudette*, after an evidentiary hearing at which the police investigator, electric company employee, and other witnesses testified, the court denied the motion to suppress, ruling that (1) the employee conducted the search largely on her own initiative, (2) that she acted primarily to prevent theft of electrical services from her private employer, not to assist in any criminal investigation, and (3) the investigator did not participate in her search. *See Gaudette*, No. 09-cr-30014-MAP (D. Mass. Sept. 6, 2011), DE #60 at 6-8.

Here, without an evidentiary hearing, this Court will be unable to make comparable factual findings. Moreover, Mr. Yu submits that witness testimony would establish that (1) ADI conducted its extensive search of Mr. Yu's devices at the FBI's request; (2) ADI acted primarily to assist the then-pending criminal investigation of Mr. Yu and his company, Tricon MMIC, not for an independent business purpose; and (3) the FBI actively participated in that search through a series of debriefing meetings with ADI.[1]

II. The warrantless search was unreasonable, because Mr. Yu had a reasonable expectation of privacy in his computer, email, and network activity.

In challenging a warrantless search, "the defendant carries the burden of making the threshold showing that he had a 'reasonable expectation of privacy in the area searched and in relation to the items seized." *United States v. Stokes*, 829 F.3d 47, 51 (1st Cir. 2016) (*quoting United States v. Aguirre*, 839 F.2d 854, 856 (1st Cir. 1988)). "The Supreme Court has set out a

[1] To the extent that ADI may have previously conducted a "private search" merely by activating its monitoring software, the scope of that search was greatly expanded at the government's behest when ADI reviewed the monitoring data and generated reports that it turned over to investigators. *See United States v. Silva*, 502 F. Supp. 2d 143, 147-48 (D. Mass. 2007) (citing *United States v. Runyan*, 275 F.3d 449, 462 (5th Cir. 2001)).

two-part test" for analyzing whether a defendant had a reasonable expectation of privacy: "first, whether the movant has exhibited an actual, subjective expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable." *United States v. Morel*, 922 F.3d 1, 8 (1st Cir. 2019) (quoting *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) (citing *Maryland v. Smith*, 442 U.S. 735, 740 (1979))). In this case, Mr. Yu satisfies that two-part test.

A. An employee can have a reasonable expectation of privacy in the workplace.

While the private home has long received special constitutional protection, *see Kyllo v. United States*, 533 U.S. 27, 31 (2001), the workplace is not a Fourth Amendment free zone. To the contrary, given the "great variety of work environments," an employee's reasonable expectations of privacy must be evaluated "on a case-by-case basis." *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). In each case, "a court must consider '[t]he operational realities of the workplace' in order to determine whether an employee's Fourth Amendment rights are implicated." *City of Ontario v. Quon*, 560 U.S. 746, 756 (2010) (quoting *O'Connor*, 480 U.S. at 717).

For example, in *City of Ontario v. Quon*, 560 U.S. 746 (2010), the Supreme Court assumed (without holding) that the warrantless search of text messages which were sent and received by a public employee, on his employer-owned and issued pager, implicated the employee's reasonable expectation of privacy. *See id.* at 765 (Stevens, J., concurring) (noting that a five-member majority in *O'Connor* agreed that "an employee enjoys a reasonable expectation of privacy in his office"). Indeed, according to the Supreme Court, it is "particularly important" to protect an employee's expectation of privacy in the workplace "in light of the 'reality of work in modern time,' which lacks 'tidy distinctions' between workplace and private activities.'" *Id.* (quoting *O'Connor*, 480 U.S. at 739 (Blackmun, J., concurring)).

B. The modern reality of invasive electronic surveillance in the private workplace is a relevant consideration.

In conducting the required "case-by-case" analysis of an employee's privacy expectations, Fourth Amendment law must reckon with the evolving reality of the modern workplace. That is the lesson of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the landmark decision holding that a person has a reasonable expectation of privacy in his historical cell-site location information.

"As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure[] the preservation of the degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Id.* at 2214 (quoting *Kyllo*, 533 U.S. at 34); *see Quon*, 560 U.S. at 759 (recognizing that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society appears to accept as appropriate behavior"). Any other approach would leave people—and their Fourth Amendment rights—"at the mercy of advancing technology." *Carpenter*, 138 S. Ct. at 2218; *see Kyllo*, 533 U.S. at 34 (requiring warrant for use of "sense-enhancing" thermal imager and refusing "to permit police technology to erode the privacy guaranteed by the Fourth Amendment").

This Court recently embraced that important principle in *United States v. Moore-Bush*, 381 F. Supp. 3d 139 (D. Mass. 2019) (allowing defendant's motion to suppress evidence from pole camera outside private home). Relying on the "necessary reasoning" of *Carpenter*, this Court recognized, "technologies that permit law enforcement officers to access and search vast amounts of passively collected data may 'give police access to a category of information otherwise unknowable,'" and, thus, raises novel Fourth Amendment concerns. *Id.* at 148 (quoting *Carpenter*, 138 S. Ct. at 2218). Although the First Circuit recently reversed the suppression decision, relying principally on *stare decisis*, *United States v. Moore-Bush*, __ F.3d __, 2020 U.S. App. LEXIS

18886 (1st Cir. June 16, 2020), this Court's legal reasoning was sound, and it applies with even greater force, here.

ADI's use of Digital Guardian to conduct an extensive digital search of Mr. Yu's computer, e-mail, and network activities more closely resembles a cellphone company's collection of a subscriber's personal historical cell-site information (as in *Carpenter*) than an officer's observation of a homeowner's outdoor activities, with a camera from a public street (as in *Moore-Bush*) or with the naked eye from an airplane (as in *California. v. Ciraolo*, 476 U.S. 207, 213 (1986)). The electronic search in this case, unlike *Moore-Bush*, did not involve "conventional surveillance techniques and tools, such as security cameras," which the Supreme Court expressly distinguished in *Carpenter*, 138 S. Ct. at 2220, and the First Circuit previously addressed in *United States v. Bucci*, 582 F.3d 108, 116-17 (1st Cir. 2009). Nor did it involve information that Mr. Yu "knowingly expose[d] to public view." *Moore-Bush*, 2020 U.S. App. LEXIS 18886, at *3, *26 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). Indeed, the prosecution alleges (and ADI apparently asserts) that much of the information at issue was strictly confidential.

Thus, notwithstanding the current state of circuit law with regard to pole cameras in particular[2], this Court should remain "attentive . . . to the risk that new technology poses even to those 'privacies of life' that are not wholly shielded from public view." *Moore-Bush*, 2020 U.S. App. LEXIS 18886, at *41 (Barron, J., concurring) (quoting *Carpenter*, 138 S. Ct. at 2214) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); *see id.* at *50 (noting that *Carpenter* "highlight[ed] the constitutional concerns raised by law enforcement's ever-increasing capacity to

[2] Concurring in *Moore-Bush*, Judge Barron called on the First Circuit to reconsider *en banc* its decision in *Bucci* in light of the Supreme Court's decision in *Carpenter*, which elaborated on the significance of earlier Fourth Amendment decisions, such as *Kyllo*, *Riley*, and *Katz*. If the full court were to accept that invitation, it might overrule *Bucci* and affirm this Court's suppression decision (which declined to follow *Bucci*).

engage in the perfect surveillance of activities that, in a lower-tech world, were clothed in practical anonymity"); *id.* at *54 (citing "*Kyllo*'s admonitions to courts . . . not to leave privacy . . . 'at the mercy of advancing technology'") (quoting *Kyllo*, 533 U.S. at 34)). Suppressing the fruit of the *unconventional* surveillance techniques and tools used in this case would be consistent with the First Circuit's "privacy-protective approach," which demands courts "be attuned to the threats to privacy posed by new technological realities despite the absence of precedent compelling us to do so." *Id.* at *62 (quoting *United States v. Wurie*, 728 F.3d 1, 14 (1st Cir. 2013)).

Just as novel technologies—from GPS and cellphone tracking to "sense-enhancing" imaging—have provided law enforcement with powerful, new investigative tools, "[r]ecent advancements in technology have made the intrusive surveillance of workers much more achievable and economical." I. Ajunwa *et al.*, "Limitless Worker Surveillance," 105 CAL. L. REV. 735, 739 (June 2017). "Today," in the corporate world, "every e-mail, instant message, phone call, line of written code, and mouse-click leaves a digital signal," and such data "can now be inexpensively collected and mined for insights into how people work and communicate[.]" Steve Lohr, "Big Data, Trying to Build Better Workers," THE NEW YORK TIMES (Apr. 20, 2013), *available at* https://www.nytimes.com/2013/04/21/technology/big-data-trying-to-build-better-workers.html. These sweeping digital capabilities distinguish modern employer surveillance from traditional human surveillance. *See Moore-Bush*, 381 F. Supp. 3d at 149. As a result, "it is uncertain how workplace norms, and the law's treatment of them, will evolve," *Quon*, 560 U.S. at 759.

C. ADI's warrantless search violated Mr. Yu's reasonable expectation of privacy.

In this case, ADI's search, at the government's behest, was more like collecting historical cell-site location information or using a wall-penetrating thermal imager (which require warrants) than an "imperfect" human observer (which does not). *See id.* Because the search allowed the

government (or ADI, as the government's agent) to look into an area that Mr. Yu had not exposed to public view and "to piece together the intimate details of [his] life," it infringed on Mr. Yu's reasonable expectation of privacy. *Id.* at 150 (citing *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring))).

As with *Carpenter*, *Kyllo*, and *Moore-Bush*, this case raises challenging questions about powerful digital surveillance technologies that are "remarkably easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 138 S. Ct. at 2218. "With just the click of a button," modern surveillance technology, such as Digital Guardian, can "access [a] deep repository" of information about a particular employee and all of his or her digital activities, both professional and personal, in the workplace. *Id.* Because such voluminous data is historical, encyclopedic, and searchable, there is no "escape" from the potential for "tireless and absolute surveillance" in the workplace. *Id.* at 2218. Thus, it is critical to ensure that Fourth Amendment protections continue to address the privacy risks inherent in the modern digital workplace.

Precedent regarding workplace privacy counsels this Court to "proceed with care." *Quon*, 560 U.S. at 759 (recognizing the uncertainty concerning "the Fourth Amendment implications of emerging technology"). For example, in *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Supreme Court found that a doctor had a reasonable expectation of privacy in his office desk and file cabinets because they were assigned exclusively to him, he did not share them with anyone, and over the course of 17 years, other employees had never accessed them. *Id.* at 717-18. In *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001), the Second Circuit held an employee had a reasonable expectation of privacy in his office computer because his employer did not have "a general practice

of routinely conducting searches of office computers" and had not given the employee "notice that he should have no expectation of privacy in the contents of his office computer." *Id.* at 74.[3]

D. An evidentiary hearing is required to determine the "operational realities" of Mr. Yu's employment with ADI.

An evidentiary hearing is needed to develop a complete factual record for this Court to determine whether, as an employee of ADI, Mr. Yu had a reasonable expectation of privacy in his office computer, e-mail, and network activity, *see* Yu Decl. ¶ 7, and whether, as an agent of the government, ADI conducted an unreasonable search of Mr. Yu's devices and data in order to assist the government with its criminal investigation. If the record establishes ADI's search was not "necessary for a non-investigatory work-related purpose" or that it was "excessively intrusive," *Quon*, 560 U.S. at 761 (quoting *O'Connor*, 480 U.S. at 726); *see id.* at 765, this Court should conclude the warrantless workplace search was unreasonable and, thus, violated Mr. Yu's Fourth Amendment rights.

CONCLUSION

For the foregoing reasons, this Court should hold an evidentiary hearing and, thereafter, grant this motion to suppress all fruit of the warrantless search of Defendant Haoyang Yu's computer, email, and network activity.

---

[3] Even when corporations provide routine disclosures or general notices to employees about potential computer and e-mail monitoring, those measures cannot negate all Fourth Amendment protections. M. Green, "Against Employer Dumpster-Diving for Email," 64 S.C. L. REV. 323 (Winter 2012) ("The façade effectuated by adhesion policies—regarding device use—that attempt to suggest employees have no expectation of privacy in communications found on employer devices and have also consented to employer searches for employee communications found on those devices as a legal paradigm should now be clearly rejected."). An employer's "technology use policy" cannot strip its employees of any expectation of privacy any more than a cellphone company's "terms of use" can strip its customers of such expectations. At no time, when Mr. Yu accepted employment with ADI, signed standard non-disclosure agreements, or received routine employment policies, did he intend to give up all of his privacy rights or work or understand that he was doing so. *See* Yu Decl. ¶¶ 9-10.

Respectfully submitted,

HAOYANG YU

by his attorneys,

/s/ William Fick

William W. Fick (BBO #650562)
Daniel N. Marx (BBO #674523)
FICK & MARX LLP
24 Federal Street, 4th Floor
Boston, MA 02110
(857) 321-8360
wfick@fickmarx.com
dmarx@fickmarx.com

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on June 22, 2020.

/s/ William Fick